

**IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA**

## Alexandria Division

UNITED STATES OF AMERICA ) Case No. 1:19-CR-164  
v. ) The Honorable Liam O'Grady  
MICHAEL BUTLER, ) Bench Trial: September 4, 2019  
*Defendant.* )

## **GOVERNMENT'S TRIAL BRIEF**

On September 4, 2019, Michael Butler will appear for a bench trial on one count of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1), and one count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2). The government's investigation revealed that, among other things, the defendant downloaded child pornography files through an online peer-to-peer network in March 2015 and possessed other child pornography files on a Toshiba laptop from at least about February 2015 to about July 2015. This Trial Brief provides an overview of how the United States will prove beyond a reasonable doubt that the defendant committed these acts and addresses evidentiary issues that may arise at trial.

Respectfully submitted,

G. Zachary Terwilliger  
United States Attorney

Date: August 28, 2019

By: /s/

William G. Clayman  
Special Assistant United States Attorney (LT)  
Carina A. Cuellar  
Assistant United States Attorney

## TABLE OF CONTENTS

BACKGROUND .....	4
FACTUAL SUMMARY OF THE GOVERNMENT'S CASE.....	5
I.    A Child Pornography Investigation Leads the Federal Bureau of Investigation to the Defendant's Home .....	5
II.    The Defendant Confesses to Viewing Child Pornography Online and the FBI Seizes his Laptops.....	5
III.    A Forensic Examination of the Defendant's Laptops Reveals Child Pornography and the Defendant's Use of the BitTorrent Peer-to-Peer Network.....	6
APPLICABLE LAW .....	7
I.    Burden of Proof and Reliance on Circumstantial Evidence .....	8
II.    Essential Elements of Receipt of Child Pornography.....	8
A.    Elements One, Three, and Four – The Defendant Knowingly Received a Visual Depiction of a Minor Engaged in Sexually Explicit Conduct .....	9
B.    Element Two – The Defendant Knowingly Received Child Pornography Using Any Means or Facility of Interstate and Foreign Commerce .....	13
C.    The Defendant Also Attempted to Receive Child Pornography .....	14
III.    Essential Elements of Possession of Child Pornography.....	15
A.    The Defendant Knowingly Possessed One or More Matters that Contained a Visual Depiction of a Minor Engaged in Sexually Explicit Conduct .....	16
1.    The Defendant Possessed the Child Pornography Files on the Toshiba Laptop.....	16
2.    The Defendant Knowingly Possessed the Child Pornography Files Found on the Toshiba Laptop.....	18
EVIDENTIARY ISSUES .....	21
I.    The Defendant's Uncharged Child Pornography Offenses Are Admissible as Intrinsic Evidence and Under Federal Rules of Evidence 414 and 404(b) .....	21
A.    The Uncharged Child Pornography Offenses Should Be Admitted as Intrinsic Evidence of the Charged Conduct .....	21
B.    Evidence of the Defendant's Uncharged Child Pornography Offenses Is Also Admissible Pursuant to Federal Rule of Evidence 414 .....	23

1. Rule 414's Prerequisites for Admitting Evidence of Uncharged Acts of Child Molestation Are Met Here .....	24
2. The Probative Value of the Proffered Rule 414 Evidence Is Not Substantially Outweighed by the Danger of Unfair Prejudice .....	27
C. The Uncharged Child Pornography Offenses Are Admissible Under Rule 404(b) to Show Identity, Knowledge, Opportunity, Intent, and Lack of Mistake.....	30
II. The Court Can Determine that the Child Pornography Depicts Real Minors Engaged in Sexually Explicit Conduct .....	34
CONCLUSION.....	35

## BACKGROUND

The defendant's case is a familiar one, complicated primarily by the repeated use of anti-forensics computer software designed to wipe evidence from various areas of the defendant's Toshiba laptop's computer system. Despite the defendant's use of this software, however, the government's investigation uncovered evidence establishing that, in March 2015, the defendant searched for and downloaded child pornography online through the BitTorrent peer-to-peer network.<sup>1</sup> The government's investigation also established that, from at least about February 2015 to about July 2015, the defendant stored digital child pornography files on his laptop.

As explained below, these facts are based primarily on the defendant's voluntary admissions to law enforcement during the July 2015 search of his home and a forensic examination of the defendant's computer devices seized during that search. The government will prove these facts beyond a reasonable doubt over the course of a one-day trial by calling around two witnesses, including law enforcement personnel involved in the execution of the search warrant and a digital investigative analyst who forensically examined the defendant's seized devices.<sup>2</sup>

---

<sup>1</sup> The term "child pornography" will be used in this Trial Brief to refer to visual depictions of minors engaged in sexually explicit conduct, as those terms are defined in 18 U.S.C. § 2256.

<sup>2</sup> The parties have discussed a number of stipulations, including stipulations to: the defendant's residency within the Eastern District of Virginia; the defendant's ownership of the devices seized from his home in July 2015; the assembly location of the defendant's Toshiba laptop; the chain of custody of the seized devices; and the accuracy of the forensic images of the devices that were used for examination by the digital investigative analyst. Any agreements to stipulations will be promptly filed with the Court.

## **FACTUAL SUMMARY OF THE GOVERNMENT'S CASE**

### **I. A Child Pornography Investigation Leads the Federal Bureau of Investigation to the Defendant's Home**

In February 2015, the Federal Bureau of Investigation (“FBI”) arrested the administrator a child pornography website that operated on an anonymous online service known as The Onion Router (or “Tor”). After the arrest, the FBI initiated a plan to locate the site’s members by briefly assuming control of the site and deploying a computer code that would reveal the IP address of members who accessed content on the site. One such IP address revealed through this investigation was then traced by law enforcement to a family residence in Sterling, Virginia, which is within the Eastern District of Virginia. On July 8, 2015, FBI Special Agent (“SA”) Peter Kaupp obtained a warrant from the U.S. District Court for the Eastern District of Virginia to search this home for child-pornography-related evidence.

### **II. The Defendant Confesses to Viewing Child Pornography Online and the FBI Seizes his Laptops**

On July 9, 2015, law enforcement executed the warrant. At the time, the defendant, then 23 years old, lived in the home with his mother and father, though only the defendant and his mother were present during the search. While law enforcement searched the premises, the defendant agreed to speak with SA Kaupp and FBI SA Tonya Sturgill Griffith in the furnished sitting area in the basement of the home. During the interview, the defendant told the SAs that he had a Toshiba laptop computer for personal use and that he was the only person who used or had access to the device. When asked if he had heard of Tor before, the defendant acknowledged that he had and described it as “sites that . . . don’t show up with Google basically.” He told the SAs that he downloaded Tor about a year prior to the search out of curiosity, but later elaborated that he used Tor to look at child pornography with a specific interest in child pornography depicting

girls. When asked what websites he visited using Tor to look at child pornography, the defendant said that he did not know because “everything is so encrypted.” The defendant also told the SAs that, in 2010, he used a peer-to-peer (“P2P”) network to access child pornography and was later arrested by law enforcement for this conduct.

At the end of the search, law enforcement seized several devices from the home, including a Toshiba Satellite C75DB7100 laptop (serial number: ZE029171U) with a Toshiba 750 GB hard drive (serial number: 9422T1CZT) (“the Toshiba laptop”) from the defendant’s bedroom and a Dell Latitude E6510 laptop (service code: 21282402169) with a Seagate Momentus 7200 250 GB hard drive (serial number: 5VG5WZP0) (“the Dell laptop”) from the basement of the home.

### **III. A Forensic Examination of the Defendant’s Laptops Reveals Child Pornography and the Defendant’s Use of the BitTorrent Peer-to-Peer Network**

After law enforcement seized the Toshiba laptop and the Dell laptop from the defendant’s home, the FBI transferred custody of the unaltered devices to the Child Exploitation and Obscenity Section of the Criminal Division of the Department of Justice, where Dero Tucker, a Digital Investigative Analyst (“DIA”) in the High Technology and Investigative Unit, forensically examined them. On August 20, 2019, the United States filed with the Court and provided to defense counsel notice of its intent to introduce expert testimony at trial. *See* Notice Under Rule 16(a)(1)(G), Dkt. 44. The United States expects to call as a witness at trial DIA Tucker, who will testify about his forensic examination of the Toshiba laptop and the Dell laptop. As the government explained in its notice of intent to introduce evidence of the defendant’s prior child pornography offenses, DIA Tucker is expected to testify regarding the defendant’s use of the Dell laptop to receive child pornography in 2011 and 2012. *See* Notice of Intent to Introduce Certain Evidence Pursuant to Federal Rule of Evidence 414, Dkt. 43. It is also anticipated that DIA Tucker’s testimony will prove that images and videos of child pornography were stored on the

Toshiba laptop from at least February 2015 to July 2015, and that the defendant used the device to download and attempt to download child pornography through the BitTorrent P2P file-sharing network in March 2015.

By way of background, P2P file sharing is a method of online communication available to users of special P2P file-sharing programs. P2P file-sharing programs allow groups of computer users using the same file-sharing network to connect with and download files from each other. BitTorrent is the name of one such network. Users can connect to the BitTorrent network through certain publicly-available programs—including one called uTorrent, for example—and use what are known as “torrent” files to download content from other users connected to the network. A torrent file is a small file that contains information about one or more other, different files that a BitTorrent user may be trying to download. A torrent file does not contain the content associated with the other file or files—that is, the images or videos that a user may be trying to download. Rather, it only serves to provide instructions as to how to download that content from other BitTorrent users who are sharing it. Once a BitTorrent user uses the torrent file with a program like uTorrent, the uTorrent program will automatically download pieces of the associated content file or files from other BitTorrent users who are sharing it to the original BitTorrent user’s computer. For example, a BitTorrent user looking to download a movie can search the internet for a torrent file associated with that movie, download the torrent file, and use that torrent file with a program like uTorrent to download the movie to their computer from other BitTorrent users.

#### **APPLICABLE LAW**

The indictment charges the defendant with (1) knowingly receiving and attempting to receive child pornography via a peer-to-peer network in or about March 2015 and (2) knowingly possessing and attempting to possess at least one matter—namely, a Toshiba laptop—containing

one or more different digital visual depictions of child pornography from at least in or about February 2015 to in or about July 2015. *See* Indictment, Dkt. 22.

**I. Burden of Proof and Reliance on Circumstantial Evidence**

The government bears the burden of proving the defendant's actual and attempted receipt and possession of child pornography beyond a reasonable doubt. This standard, however, does not require proof to an absolute certainty. As the Fourth Circuit has explained, the government must prove its case beyond a *reasonable* doubt, "not 'beyond all possible doubt.'" *United States v. Adkins*, 937 F.2d 947, 950 (4th Cir. 1991). Nor does the beyond-a-reasonable-doubt standard require the government to prove its case solely through direct evidence. The Fourth Circuit has "observed repeatedly [that] 'circumstantial evidence is not inherently less valuable or less probative than direct evidence' and may alone support a guilty verdict" in criminal cases. *United States v. Martin*, 523 F.3d 281, 289 (4th Cir. 2008) (quoting *United States v. Williams*, 445 F.3d 724, 731 (4th Cir. 2006)). The government may also ask the Court as factfinder to use its power of deduction and inference to draw reasonable inferences from the circumstantial evidence presented at trial to obtain a conviction of the defendant. *See United States v. Ashley*, 606 F.3d 135, 140 (4th Cir. 2010) ("[W]hile it is important that we not permit a verdict based solely on the piling of inference upon inference, it is also imperative that we not rend the fabric of evidence and examine each shred in isolation.") (quoting *United States v. Johnson*, 903 F.2d 1084, 1087 (7th Cir.1990)).

**II. Essential Elements of Receipt of Child Pornography**

Count One of the indictment alleges that the defendant received child pornography in or about March 2015. To obtain a conviction on this count, the United States must prove the following essential elements beyond a reasonable doubt:

- (1) The defendant knowingly received any visual depiction;
- (2) The defendant did so using any means or facility of interstate or foreign commerce;
- (3) The production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, and the visual depiction was of such conduct; and
- (4) The defendant knew that the visual depiction involved the use of a minor engaging in sexually explicit conduct.

*See 18 U.S.C. § 2252(a)(2); see also United States v. Cedelle, 89 F.3d 181, 185 (4th Cir. 1996).*

**A. Elements One, Three, and Four – The Defendant Knowingly Received a Visual Depiction of a Minor Engaged in Sexually Explicit Conduct**

While the relevant statute does not define what it means to *knowingly receive* child pornography, courts generally adopt “the common-sense understanding of the term.” *United States v. Osborne*, 935 F.2d 32, 34 n.2 (4th Cir. 1991) (citing *United States v. Flippin*, 861 F.2d 266 (4th Cir. 1988)); *see also United States v. Ramos*, 685 F.3d 120, 131 (2d Cir. 2012) (“The statute does not define receipt or possession, and courts have given these terms their plain meaning.”). The “ordinary meaning of ‘receive’ is ‘to knowingly accept’; ‘to take possession or delivery of’; or ‘to take in through the mind or sense.’” *United States v. Pruitt*, 638 F.3d 763, 766 (11th Cir. 2011) (quoting *Webster’s Third New International Dictionary: Unabridged* 1894 (1993)). Thus, “[a] person ‘knowingly receives’ child pornography [] when he intentionally views, acquires, or accepts child pornography on a computer from an outside source.” *Id.*; *see also Osborne*, 935 F.2d at 34 n.2 (observing that a defendant knowingly received child pornography videos when he “achieved the power to exercise dominion and control over them”); *United States v. Mohrbacher*, 182 F.3d 1041, 1048 (9th Cir. 1999) (“An individual who downloads material takes possession or accepts delivery of the visual image; he has therefore certainly received it.”). And while a number of factors might establish that a defendant took the requisite steps to

knowingly receive child pornography, none is talismanic. *United States v. Winkler*, 639 F.3d 692, 698 (5th Cir. 2011). Instead, the inquiry should be “highly fact specific” so as to “comport[] with the ordinary, everyday meaning of the word ‘receive’” and “prevent[] savvy users of child pornography from using the technologically static nature of [judicial] opinions as a basis for engaging in precisely the behavior the anti-child pornography statutes were meant to forbid.” *Id.*<sup>3</sup> To be sure, though, there is “no . . . question” that a defendant knowingly received child pornography “where [he] actively used a computer to solicit obscene material through numerous and repetitive searches and ultimately succeeded in obtaining the materials he sought.” *United States v. Whorley*, 550 F.3d 326, 334 (4th Cir. 2008).

The knowledge requirement here also extends to the defendant’s “knowledge of ‘the sexually explicit nature of the materials as well as . . . the involvement of minors in the materials’ production . . .’” *United States v. Miltier*, 882 F.3d 81, 86 (4th Cir. 2018) (quoting *United States v. Matthews*, 209 F.3d 338, 351 (4th Cir. 2000)). The United States does not, however, have to

---

<sup>3</sup> In order to grapple with the technological sophistication of many online consumers of child exploitation material, courts have taken steps to delineate the types of forensic evidence that show a defendant’s knowing receipt of child pornography. *See, e.g., United States v. Myers*, 560 F. App’x 184, 186 (4th Cir. 2014) (per curiam) (“[A] defendant’s attempts to delete a computer’s temporary internet files and browsing history are circumstantial evidence supporting knowing receipt of child pornography, given that a defendant’s scrubbing of the evidence indicates some degree of prior awareness that images viewed online would be saved to his computer.”); *United States v. Pawlak*, --- F.3d ---, 2019 WL 3822142, at \*9 (5th Cir. 2019) (finding evidence sufficient to support a conviction for receipt of child pornography where thumbnail files of child pornography were found on the defendant’s computer and he admitted to being a long-time consumer of child pornography and a member of Playpen); *United States v. Schaff*, 454 F. App’x 880, 882 (11th Cir. 2012) (finding evidence sufficient to support conviction for receipt of child pornography where defendant intentionally deleted child pornography from his computer and law enforcement discovered thumbnail images of child pornography in user-controlled folders on the defendant’s laptop); *Pruitt*, 638 F.3d at 766 (“Evidence that a person has sought out—searched for—child pornography on the internet and has a computer containing child-pornography images—whether in the hard drive, cache, or unallocated spaces—can count as circumstantial evidence that a person has ‘knowingly receive[d]’ child pornography.”).

prove “that the defendant knew the [child pornography] material was in fact illegal at the time of receipt.” *United States v. Silva*, 794 F.3d 173, 182 (1st Cir. 2015) (internal citation omitted). Rather, it only needs to prove that the defendant generally knew of “the facts that make his conduct fit the definition of the offense[.]” *Id.* (citing *Elonis v. United States*, 135 S.Ct. 2001, 2009 (2015)); *see also United States v. Wellman*, 663 F.3d 224, 230–31 (4th Cir. 2011) (recognizing that, under § 2252, “a defendant’s knowledge of the law is not a relevant consideration”); *United States v. Knox*, 32 F.3d 733, 754 (3d Cir. 1994) (“[T]o fulfill the knowledge element of § 2252, a defendant simply must be aware of the general nature and character of the material and need not know that the portrayals are illegal.”).<sup>4</sup> Given the nature of child pornography offenses, such knowledge is often established through circumstantial evidence, including the presence and amount of child pornography files on a defendant’s computer, the titles of the files of child pornography, the defendant’s ability to access the child pornography, and the frequency with which the defendant engaged in this activity. *Myers*, 560 F. App’x at 186–87; *United States v. Freeman*, 1:14-CR-322 (JCC), 2015 WL 45521, at \*8–10 (E.D. Va. Jan. 2, 2015).

To prove that the defendant here knowingly received child pornography in March 2015, the government intends to present evidence establishing that he was the sole user of a password-protected Toshiba laptop on which he had installed the uTorrent P2P file-sharing program under an account associated with the username “Michael Butler.” The forensic evidence will show that on the night of March 8, 2015, the defendant accessed a website using a username associated with him and that very shortly after that, he accessed various other websites on which he could search

---

<sup>4</sup> The defendant in *Knox* argued, in part, that “although he knew the contents of the . . . tapes, he was unaware that the videos were child pornography and believed they were legal to own.” 32 F.3d at 753. The appellate court rejected that argument and concluded: “The child pornography laws would be eviscerated if a pedophile’s personal opinion about the legality of sexually explicit videos was transformed into the applicable law.” *Id.* at 754.

for and download torrent files. The United States anticipates that the evidence will show that the defendant repeatedly searched these sites for torrent files using terms associated with child pornography, including references to known series of child pornography. The forensic evidence will also show that in this same timeframe, the defendant downloaded about 37 torrent files, many of which have titles that are similar or identical to the torrent files he was searching for, and accessed the uTorrent program multiple times. The forensic evidence will show that the uTorrent program was configured to save downloaded content to the “Downloads” folder under the “Michael” user account on the laptop, and that over a dozen thumbnail image files depicting child pornography or the titles of child pornography torrent files that the defendant downloaded between March 8 and 9, 2015, were recovered from this “Downloads” folder. The United States also anticipates the forensic evidence establishing that a child pornography video was recovered from the unallocated space of the laptop. The United States intends to show that this video file begins by displaying the name of a torrent file that the defendant downloaded between March 8 and 9, 2015, and then shows what appears to be minor girls in various stages of undress, including at least one shot focused on the exposed, nude vagina of what appears to be a minor girl. The United States also intends to show that the defendant conducted similar searches for child-pornography-related torrent files using the Toshiba laptop on March 30, 2015. The United States submits that these proffered facts, which show that the defendant repeatedly searched for and ultimately obtained child pornography on his laptop, are by themselves sufficient to establish that he knowingly received child pornography in March 2015. *See Whorley*, 550 F.3d at 334.

As additional evidence establishing his knowledge, the United States intends to show that the defendant repeatedly used an application designed to scrub forensic artifacts from his Toshiba laptop between April and July 2015, and that hundreds of accessible images and videos of child

pornography or child erotica were discovered on the device. The government also intends to show that two child pornography video files that the defendant deleted before the search of his home were recovered from the Recycle Bin of the laptop, and that forensic artifacts show that he viewed at least one of the videos before deleting it. Relatedly, the government anticipates eliciting testimony that during the July 2015 search of his home, the defendant told law enforcement that he had been viewing child pornography online for about a year prior to the search and that he had previously accessed child pornography using a P2P file-sharing program in 2010. The government expects to confirm the defendant's admitted prior child-pornography-related activity by presenting computer forensic evidence obtained from a Dell laptop that was also seized from the defendant's home. The government anticipates that this evidence will show that, in 2011, the defendant used it to search for and download torrent files with titles indicative of child pornography. The government further anticipates that the forensic evidence from the Dell laptop will show that the defendant used BitLord, which is another P2P file-sharing program, on the device and that, in 2012, he repeatedly accessed videos and images with explicit, child-pornography-related titles from a folder that stored files downloaded from BitLord. The government also expects the evidence to show that child pornography files were located in the unallocated space of this laptop.

**B. Element Two – The Defendant Knowingly Received Child Pornography Using Any Means or Facility of Interstate and Foreign Commerce**

Section 2252(a)(2) requires that the defendant commit the crime using a “facility or means of interstate . . . commerce[.]” It is well established that the transmission of images or video content by means of the internet constitutes the use of a facility of interstate commerce. *See Miltier*, 882 F.3d at 87–88 (“Courts, including this one, have repeatedly held that use of the internet in transmission of child pornography satisfies the interstate commerce element of the offense.”); *Jeffries v. United States*, No. 4:15-CR-83 (MSD), 2018 WL 4903267, at \*4 (E.D. Va. Oct. 9, 2018)

(“[E]very court to address the issue agrees with the unremarkable proposition that the Internet is a means of interstate commerce[.]” (internal citation and quotations omitted)) (collecting cases).

Here, the United States intends to introduce forensic evidence establishing that the defendant used the internet to search for and download torrent files related to child pornography, and then further used the internet to download the associated child pornography over the BitTorrent P2P network. Accordingly, this element is satisfied for Count One.

### **C. The Defendant Also Attempted to Receive Child Pornography**

The United States further alleges in Count One that the defendant attempted to receive child pornography in or about March 2015. To convict the defendant of attempted receipt of child pornography, the government must prove beyond a reasonable doubt that he (1) “had culpable intent to commit the crime and (2) . . . took a substantial step towards completion of the crime that strongly corroborates that intent.” *United States v. Engle*, 676 F.3d 405, 419 (4th Cir. 2012) (citing *United States v. Neal*, 78 F.3d 901, 906 (4th Cir. 1996)). A defendant takes a substantial step when he “puts in motion events that would, from the defendant’s point of view, result in the commission of a crime but for some intervening circumstance.” *United States v. Pratt*, 351 F.3d 131, 135 (4th Cir. 2003). A “substantial act toward the commission of a crime need not be the last possible act before its commission.” *Id.* Rather, “[a]n attempt comprises any substantial act in a progression of conduct that is meant to culminate in the commission of the crime intended.” *Id.*

For the charged offense, evidence of a defendant’s culpable intent to commit the crime can include his internet search terms, the names of any child pornography files he attempted to receive, evidence that he sought to control child pornography files in a manner that goes beyond passive viewing, and prior child-pornography-related activity. *United States v. Eychaner*, 326 F. Supp. 3d 76, 86–89 (E.D. Va. 2018); *see also United States v. Gartenlaub*, Case No. 14-173, 2016 WL

3607154, at \*4 (C.D. Cal. June 30, 2016) (finding that jury could have inferred defendant intended to download child pornography based on the names of the files that he partially downloaded). Likewise, proof that a defendant took a substantial step towards the completion of the offense can be established through evidence that he initiated the process of downloading what he knew was a child pornography file or that he navigated to sites that would allow him to download child pornography. *See Eychaner*, 326 F. Supp. 3d at 89; *Gartenlaub*, 2016 WL 3607154, at \*4 (finding that jury could have inferred defendant took substantial step towards receiving child pornography by clicking on files with names indicative of child pornography).

Here, the government anticipates presenting evidence establishing that, in March 2015, the defendant repeatedly navigated to sites from which he could download torrent files, searched for torrent files using terms related to child pornography, and downloaded dozens of torrent files at the same time. The United States further expects to elicit testimony that the purpose of a torrent file is to download the associated content using the BitTorrent P2P network. Further, and as discussed in more detail above, the United States intends to present evidence that the defendant admitted to accessing child pornography online and through P2P software, as well as forensic evidence that the defendant searched for, downloaded, and viewed child pornography using the BitTorrent P2P network in 2011 and 2012. The United States submits that these proffered facts, taken together, leave no question that in March 2015 the defendant intended to receive child pornography and took several substantial steps towards the completion of that offense.

### **III. Essential Elements of Possession of Child Pornography.**

Count Two alleges that, between about February 2015 and about July 2015, the defendant knowingly possessed and attempted to possess on his Toshiba laptop child pornography distinct

from the content he received in March 2015. To obtain a conviction, the United States must prove the following essential elements beyond a reasonable doubt:

- (1) The defendant knowingly possessed at least one matter that contained a visual depiction of a minor engaged in sexually explicit conduct;
- (2) The production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, and the visual depiction was of such conduct;
- (3) The defendant knew that the visual depiction involved the use of a minor engaging in sexually explicit conduct; and
- (4) The visual depiction had been mailed, shipped, or transported using any means or facility of interstate or foreign commerce, or had been shipped or transported in or affecting interstate or foreign commerce, or was produced using materials that had been mailed, shipped, or transported using any means or facility of interstate or foreign commerce, including by computer.<sup>5</sup>

*See* 18 U.S.C. § 2252(a)(4)(B).

**A. The Defendant Knowingly Possessed One or More Matters that Contained a Visual Depiction of a Minor Engaged in Sexually Explicit Conduct**

**1. The Defendant Possessed the Child Pornography Files on the Toshiba Laptop**

It is axiomatic that to possess an item is to exercise control or authority over it. “The law recognizes two kinds of possession: actual possession and constructive possession. *United States v. Penniegraft*, 641 F.3d 566, 572 (4th Cir. 2011). The former is the “physical . . . control over

---

<sup>5</sup> Section 2252(a)(4)(B) provides for federal jurisdiction where the child pornography was “produced using materials [that] have been mailed or . . . shipped or transported” in interstate or foreign commerce or affecting in state or foreign commerce. Because “pornographic images [are] ‘produced’ . . . when they [are] copied to [a] . . . computer,” *United States v. Caley*, 355 F. App’x 760, 761 (4th Cir. 2009) (per curiam), the government can establish this element by showing that the medium housing the child pornography was manufactured in another state or overseas, *United States v. Guagliardo*, 278 F.3d 868, 870-71 & n.2 (9th Cir. 2002). Here, this can be established through evidence that the defendant’s Toshiba laptop was manufactured outside the state of Virginia. *See United States v. Scott*, No. 2:13-CR-164, 2014 WL 2808802, at \*4 (E.D. Va. Jun. 20, 2014) (holding in a child pornography prosecution that “Made in China” and “Made in Korea” inscriptions on cellphones were self-authenticating under Federal Rule of Evidence 902(7), were not hearsay statements, and were admissible).

property,”” *id.* (quoting *United States v. Scott*, 424 F.3d 431, 435 (4th Cir. 2005)), while the latter exists where an individual “has ownership, dominion, or control over the contraband itself or over the premises or vehicle in which it was concealed,”” *id.* at 572 (quoting *United States v. Armstrong*, 187 F.3d 392, 396 (4th Cir. 1999)). Numerous federal courts, including the Fourth Circuit, have recognized that § 2252 criminalizes both the actual and constructive possession of child pornography. *See, e.g.*, *United States v. Moreland*, 665 F.3d 137, 149 (5th Cir. 2011); *United States v. Osborne*, 935 F.2d 32, 34 n.2 (4th Cir. 1991).

Actual and constructive possession of child pornography “may be proven by direct or circumstantial evidence.” *United States v. Smith*, 739 F.3d 843, 846 (5th Cir. 2014). As this Court has observed in the context of a receipt prosecution, a lack of “direct evidence that places [a] [d]efendant at the . . . desktop downloading and viewing child pornography. . . . is not dispositive or even required . . . .” *United States v. Freeman*, No. 1:14-CR-322 (JCC), 2015 WL 45521, at \*9 (E.D. Va. Jan. 2, 2015). Rather, the Court as factfinder may properly consider the totality of the circumstances surrounding the defendant’s alleged possession. *United States v. Herder*, 594 F.3d 352, 358 (4th Cir. 2010).

At trial, the government will prove that the defendant possessed the child pornography found on the Toshiba laptop seized from his bedroom. As an initial matter, the government expects the evidence to show that the defendant voluntarily admitted that he was the sole user of a password-protected Toshiba laptop. The United States also expects to present forensic evidence confirming that the Toshiba laptop on which child pornography was stored was password-protected, and that the password provided by the defendant allowed the forensic examiner to access the “Michael Butler” user account. The government intends to elicit testimony that child pornography files were discovered in multiple locations, including several accessible locations, on

the Toshiba laptop under the “Michael” user account. Specifically, the United States intends to present evidence about the following:

- A child pornography video titled “3rd\_grade\_and\_already\_bating.avi” stored in a folder titled “boneheads23772” in the “Documents” folder of the “Michael” user account that depicts what appears to be a minor girl touching and exposing her vagina;
- Dozens of child pornography images under the “Michael” user account in a folder associated with OneDrive, which is a cloud-based file storage service offered by Microsoft that allows users to store and sync files online, including multiple images that depict what appears to be an adult male engaging in oral and vaginal sex with a prepubescent girl;
- Two videos of child pornography recovered from the Recycle Bin of the device. One video, titled “Alicia.mpg,” is approximately 14 minutes long and depicts what appears to be an adult male engaging in oral and anal sex with a prepubescent girl. The other video, titled “LO5.flv,” is approximately 27 minutes long and depicts, among other things, what appears to be an adult male engaging in oral sex with a minor girl. Forensic evidence on the laptop shows that the defendant viewed the video titled “LO5.flv” on about July 8, 2015, before deleting it.

The government submits that these proffered facts alone establish the requisite nexus for finding that the defendant had possession over the files of child pornography on the Toshiba laptop.

## **2. The Defendant Knowingly Possessed the Child Pornography Files Found on the Toshiba Laptop**

With respect to the knowledge element of § 2252(a)(4), the government is not required to prove that the defendant knew that possessing child pornography was prohibited by law. The government, instead, need only prove that the defendant believed the files he possessed were child pornography. *See, e.g., United States v. Wellman*, 663 F.3d 224, 230–31 (4th Cir. 2011) (recognizing that, under § 2252, “a defendant’s knowledge of the law is not a relevant consideration”); *United States v. Knox*, 32 F.3d 733, 754 (3d Cir. 1994) (“Therefore, to fulfill the knowledge element of § 2252, a defendant simply must be aware of the general nature and character of the material and need not know that the portrayals are illegal.”). Courts confronting

the question of whether a defendant knowingly possessed child pornography generally consider at least the following four factors:

(1) whether the images were found on the defendant's computer; (2) the number of images of child pornography that were found; (3) whether the content of the images was evident from their names; and (4) [the] defendant's knowledge of[,] and ability to[,] access the storage area for the images.

*United States v. Miller*, 527 F.3d 54, 67 (3d Cir. 2008) (citing *United States v. Irving*, 452 F.3d 110, 122 (2d Cir. 2006); *see also United States v. Romm*, 455 F.3d 990, 997–1001 (9th Cir. 2006); *United States v. Payne*, 341 F.3d 393, 403 (5th Cir. 2003)); *United States v. Myers*, 560 F. App'x 184, 187–88 (4th Cir. 2014) (per curiam) (discussing similar considerations in affirming conviction for receipt, transportation, and possession of child pornography); *Freeman*, 2015 WL 45521, at \*8 (applying the four-factor test set forth in *Miller* in a receipt prosecution). At trial, the government will produce evidence that each of these four factors supports the conclusion that the defendant knowingly possessed child pornography.

**a. Factors 1–3: Dozens of Files of Child Pornography Were Found on the Defendant's Toshiba Laptop, Including a File with a Name Indicative of Child Pornography**

As for the first three factors, the government expects that the evidence will establish that the Toshiba laptop contained dozens of files of child pornography. *See, e.g., United States v. Stanley*, 533 Fed. App'x 325, 328 (4th Cir. 2013) (finding knowing receipt of child pornography based in part on evidence that the defendant possessed hundreds of child pornography files); *Irving*, 452 F.3d at 121–22 (finding defendant's possession of 76 images of child pornography relevant to determination of knowing receipt); *Freeman*, 2015 WL 45521 at \*9 (similar). Further,

the evidence will show that at least one of the video files had a title—“3rd\_grade\_and\_already\_bating.avi”<sup>6</sup>—that is indicative of child pornography.<sup>7</sup>

**b. Factor 4: The Defendant Had Knowledge of and the Ability to Access the Toshiba Laptop**

With respect to the fourth and final factor, the government intends to adduce evidence at trial that the defendant had knowledge of and the ability to access the Toshiba laptop. *See e.g., Miller*, 527 F.3d at 68 (defendant’s access to the child pornography images supported jury’s verdict that defendant knowingly received child pornography). During the July 2015 search of his home, the defendant admitted that he had a Toshiba laptop that he used as his personal computer, that he was the only individual who had access to and used the laptop, and that the device was password-protected. The defendant also voluntarily provided the password to the Toshiba laptop to law enforcement, and the password the defendant provided was used to successfully log in to the device under an account with the username “Michael Butler.” Further, once in the “Michael” user account, the child pornography files were easily accessible and viewable. Indeed, at least one video was saved in a folder titled “boneheads23772” that was located immediately within the “Documents” folder of the account. It thus is reasonable to conclude that the defendant had knowledge of and the ability to access the child pornography on the thumb drive.

---

<sup>6</sup> The government intends to elicit testimony that the term “bating” is an abbreviation of the word masturbating.

<sup>7</sup> Other courts have concluded that possessing child pornography with file names indicative of their content is strong evidence supporting knowledge. *See, e.g., United States v. Breton*, 740 F.3d 1, 14 (1st Cir. 2014) (“The presence of files with names indicative of child pornography—even absent further proof of what, if anything, those files contained—tends to make it more probable that [the defendant] knowingly was involved with child pornography.”); *United States v. Carani*, 492 F.3d 867, 873–74 (7th Cir. 2007) (rejecting defendant’s argument that “any child pornography videos he may have downloaded to his computer were downloaded solely through inadvertence[,]” in part because “many files that were, or had once been, on [the defendant’s] computer had words associated with child pornography[.]”).

## **EVIDENTIARY ISSUES**

The parties have discussed possible stipulations and any forthcoming agreements to specific facts will be promptly filed with the Court. The government nevertheless anticipates that legal issues may arise at trial. Although several of them are addressed below, the government respectfully reserves the right to supplement its position.

### **I. The Defendant's Uncharged Child Pornography Offenses Are Admissible as Intrinsic Evidence and Under Federal Rules of Evidence 414 and 404(b)**

Out of an abundance of caution, the government provided notice under Rule 414 of the Federal Rules of Evidence that it intends to admit at trial evidence that the defendant received child pornography in 2010 and again from 2011 to 2012, and accessed child pornography on Tor in 2015. The government incorporates by reference its notice, which was filed on August 16, 2019. This section provides additional legal argument as to why the defendant's uncharged child pornography violations are admissible as intrinsic evidence, or alternatively under either Federal Rule of Evidence 414 or 404(b).

#### **A. The Uncharged Child Pornography Offenses Should Be Admitted as Intrinsic Evidence of the Charged Conduct**

The Fourth Circuit has instructed that evidence is intrinsic, and therefore not subject to Rule 404, if it is "an essential part of the crimes on trial, or . . . furnishes part of the context of the crime." *United States v. Queen*, 132 F.3d 991, 998 (4th Cir. 1997); *cf. United States v. Basham*, 561 F.3d 302, 326 (4th Cir. 2009) (internal citations omitted) (noting that "[e]vidence of uncharged conduct is not 'other crimes' evidence subject to Rule 404 if the uncharged conduct 'arose out of the same series of transactions as the charged offense, or if [evidence of the uncharged conduct] is necessary to complete the story of the crime on trial.'"). Here, the defendant's uncharged child

pornography offenses are direct evidence of the charged crimes and thus not evidence of “*prior bad acts*.”

In particular, Count One charges that the defendant knowingly received and attempted to receive child pornography in March 2015. As noted above, this charge will be supported by forensic evidence showing that the defendant searched for and downloaded child pornography on at least March 8 and 9, 2015, using the BitTorrent P2P network. Count Two, on the other hand, charges the defendant with possessing child pornography from February 2015 to July 2015. Importantly, Count Two is not limited to any particular file or dates of download. Rather, Count Two encompasses all images and videos contained on the defendant’s Toshiba laptop (except for those received in or about March 2015 as referenced in Count One).

Charging conduct broadly as the government has done is appropriate where, as here, the defendant’s actions can “be characterized as part of a single, continuing scheme.” *United States v. Afsharjavan*, 2015 WL 5638099, at \*4 (E.D. Va. 2015); *see United States v. Kamalu*, 298 F. App’x 251, 254–55 (4th Cir. 2008) (noting that “two or more acts, each of which would constitute an offense standing alone and which therefore could be charged as separate counts of an indictment, may instead be charged in a single count if those acts could be characterized as part of a single, continuing scheme.”); *United States v. Berardi*, 675 F.2d 894, 898 (7th Cir. 1982) (“[FRCP 7(c)(1)] necessarily contemplates that two or more acts, each one of which would constitute an offense standing alone, may be joined in a single count without offending the rule against duplicity. The line between multiple offenses and multiple means to the commission of a single continuing offense is often a difficult one to draw. The decision is left, at least initially, to the discretion of the prosecution.”).

At trial, the government expects to show that the defendant repeatedly sought out child pornography on the internet and stored child pornography on his Toshiba laptop, but also that he was a sophisticated consumer of child pornography who routinely deleted the illegal content from his laptop and used computer programs designed to cover his tracks. The defendant's uncharged child pornography offenses are therefore direct evidence that his receipt and possession of child pornography in 2015, as well as his efforts to conceal his consumption of child pornography on his Toshiba laptop, were knowing and the result of his own intentional actions. Thus, while some of the uncharged offenses predate the conduct relevant to the criminal charges, they nevertheless provide context that is "intrinsic to the story of the crime" and should be admitted as such. *United States v. Cooper*, 482 F.3d 658, 663 (4th Cir. 2007).

**B. Evidence of the Defendant's Uncharged Child Pornography Offenses Is Also Admissible Pursuant to Federal Rule of Evidence 414**

Enacted as part of the Violent Crime Control and Law Enforcement Act of 1994, Federal Rule of Evidence 414 governs the admission of evidence of similar crimes in child sex offense cases. Rule 414(a) provides, in pertinent part, that "[i]n a criminal case in which the defendant is accused of an offense of child molestation, evidence of the defendant's commission of another offense or offenses of child molestation is admissible, and may be considered for its bearing on any matter to which it is relevant." Rule 414 broadly defines the term "child molestation" to encompass not only physical contact between an adult and a child that constitutes a crime under state or federal law, but also conduct that constitutes the federal crimes of distribution, receipt, and possession of child pornography. *See* Fed. R. Evid. 414(d)(2)(B) (defining "child molestation" as a state or federal crime "involving . . . any conduct prohibited by 18 U.S.C. chapter 110"). The upshot of Rule 414 is that evidence of a defendant's prior acts of child molestation is presumptively admissible to establish the defendant's propensity to commit the charged child sex offense. Rule

414 thus stands in contrast to Federal Rule of Evidence 404(b). Although ordinarily “evidence of past crimes may not be used ‘to prove the character of a person in order to show action in conformity therewith,’” *United States v. Kelly*, 510 F.3d 433, 436 (4th Cir. 2007), Rule 414 expressly permits the admission of such propensity evidence.

In addition to the plain text of Rule 414, its legislative history shows that Congress intended Rule 414 to be an exception to the ordinary exclusion on propensity evidence. *See, e.g., United States v. Mercer*, 653 F. App’x 622, 630 (10th Cir. 2016) (citing 140 Cong. Rec. H8991-92 (1994) (“[The Rule] is critical to the protection of the public . . . [a]nd is justified by the distinctive characteristics of the cases to which it applies. In child molestation cases, for example, a history of similar acts tends to be exceptionally probative because it shows an unusual disposition of the defendant—a sexual or sado-sexual interest in children—that simply does not exist in ordinary people.”)). Rule 414, in other words, reflects Congress’s judgment that evidence of prior acts of child molestation are ““typically relevant and probative”” in child sex offense cases. *Kelly*, 510 F.3d at 436. (quoting 140 Cong. Rec. S12990 (daily ed. Sept. 20, 1994) (statement of Sen. Dole))).

**1. Rule 414’s Prerequisites for Admitting Evidence of Uncharged Acts of Child Molestation Are Met Here.**

In order to introduce at trial evidence that the defendant possessed child pornography on prior occasions, the government must make three showings. First, the government must establish that the defendant is accused of a child molestation offense. Second, the government must show that the evidence to be admitted concerns other acts of child molestation committed by the defendant. And, third, that the evidence of the defendant’s other acts of child molestation is relevant to a matter at trial. Each of these prongs is met here.

First, the indictment charges the defendant with receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1), and possession of child pornography, in violation of 18

U.S.C. § 2252(a)(4)(B) and (b)(2). Because these offenses are federal crimes set forth in Chapter 110 of Title 18 of the U.S. Code, they qualify as a “child molestation” offenses for purposes of Rule 414. *See Fed. R. Evid. 414(d)(2)(B).*

Second, the proffered Rule 414 evidence qualifies as a “child molestation” offense as that term is defined in the rule. The government intends to admit at trial evidence that the defendant received child pornography in 2010 based on his own statements, that he used uTorrent and BitLord to download and view child pornography in 2011 and 2012, and that he accessed child pornography on Tor in 2015. Such conduct constitutes crimes under Chapter 110 of Title 18 of the U.S. Code and therefore prior acts of “child molestation” under Rule 414.<sup>8</sup>

---

<sup>8</sup> The fact that the defendant was not federally convicted of this conduct is not an impediment to the introduction of this evidence under Rule 414. As numerous courts have recognized, Rule 414 permits the admission of relevant, uncharged sexual offenses. *See, e.g., United States v. Lewis*, No. 07-3143, 2009 WL 377302, at \*2 (D.C. Cir. Jan. 23, 2009) (defendant’s uncharged possession of child pornography admissible under Rule 414 in prosecution for attempted coercion and enticement of a minor); *United States v. Seymour*, 468 F.3d 378, 384–86 (6th Cir. 2006) (defendant’s prior, uncharged sexual assaults of adult females admissible under Rule 414 in case charging child molestation offenses); *United States v. Norris*, 428 F.3d 907, 913–14 (9th Cir. 2005) (defendant’s uncharged molestation of victim’s sister admissible under Rule 414). Moreover, permitting the introduction of uncharged conduct pursuant to Rule 414 accords with the Rule’s legislative history. *See* 140 Cong. Rec. H8992 (1994) (Statements by Rep. Molinari and Senator Dole) (“Evidence of offenses for which the defendant has not previously been prosecuted or convicted will be admissible . . . .”); *see also United States v. Guidry*, 456 F.3d 493, 502–03 (5th Cir. 2006) (“Because sexual assault allegations are often reduced to a swearing match, Congress aimed to assist the fact finder’s assessment of credibility through allowing evidence of the defendant’s extrinsic sexual misconduct as character or propensity evidence.”); *Johnson v. Elk Lake School Dist.*, 283 F.3d 138, 151 (3d Cir. 2002) (“Congress intended to allow admission not only of prior convictions of sexual offenses, but also of uncharged conduct”); *United States v. Mann*, 193 F.3d 1172, 1173 (10th Cir. 1999) (“[C]ourts are to ‘liberally’ admit evidence of prior uncharged sex offense . . . .”).

Relatedly, the Court is not required to make a preliminary finding that the defendant actually committed the uncharged offenses supported by the proffered Rule 414 evidence. The question of the defendant’s commission of the conduct is one of conditional relevance under Rule of Evidence 104(b), not a preliminary question of admissibility under Rule 104(a). *See Norris*, 428 F.3d at 914 (finding that Rule 104(b) governs the admissibility of Rule 414 evidence in light of the holding in *Huddleston v. United States*, 485 U.S. 681, 689 (1988), that Rule 104(b) controls

Third, the proffered evidence of other child molestation offenses is relevant to the charged conduct. Evidence is relevant “if (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action.” Fed. R. Evid. 401. Here, the defendant’s uncharged offenses—and the specific facts surrounding such conduct—is relevant to the charged offenses in two regards. As an initial matter, these other acts reflect the defendant’s longstanding sexual interest in children and the defendant’s propensity to view child pornography. And, as a result, both of these facts make it more probable that the defendant knowingly possessed and received the child pornography that law enforcement found on his Toshiba laptop in 2015. Indeed, such other conduct helps explain why the defendant knew to use computer software to remove forensic artifacts from his Toshiba laptop and cover his tracks.

In addition, because the facts surrounding the instant offense and the proffered Rule 414 conduct are nearly identical, the proffered evidence is “exceptionally probative and will certainly shed some light on the credibility of the charge and any denial by the defense.” 140 Cong. Rec. S12990 (statement of Sen. Dole) (1994). Indeed, the defendant admitted that, in 2010, he was arrested after he viewed child pornography using a P2P network. Similarly, the evidence presented at trial will demonstrate with specificity the similarities between the defendant’s instant offenses, which involved downloading child pornography over the BitTorrent P2P network, and his 2011 to 2012 conduct, which also involved downloading and viewing child pornography over the BitTorrent P2P network. Such similarities between the current and uncharged conduct give rise

---

the admission of Rule 404(b) evidence); *Johnson*, 283 F.3d at 152 (same); *United States v. Reynolds*, No. 3:11-CR-42, 2012 WL 12895042, at \*3 (S.D. Iowa Mar. 15, 2012) (same). As a result, the Court needs only to “examine[] all the evidence in the case and decide[] whether the jury [or, here, the Court as factfinder] could reasonably find the conditional[—i.e., whether the [d]efendant committed the proffered prior acts—] by a preponderance of the evidence.” *Johnson*, 283 F.3d at 152.

to a presumption of admissibility. *See Johnson*, 84 F.3d at 155 (“Where the government can show a past offense with specificity and the act is sufficiently similar to the act with which the defendant is charged, there is a presumption in favor of admissibility.”).

## **2. The Probative Value of the Proffered Rule 414 Evidence Is Not Substantially Outweighed by the Danger of Unfair Prejudice**

Although Rule 414 supersedes Rule 404’s general prohibition of evidence of character or propensity, it does not supplant other general standards under the rules of evidence. Evidence admitted under Rule 414 therefore “remains subject to the balancing test imposed by Rule 403.” *United States v. Mason*, 532 F. App’x 432, 437 (4th Cir. 2013). As a result, even if proffered evidence satisfies all of the elements for admission under Rule 414, the evidence may still “be excluded if its probative value is substantially outweighed by the danger of unfair prejudice to the defendant.” *Id.* (internal quotations and citations omitted).

Yet, as several courts have recognized, Rule 414 necessarily alters the typical operation of Rule 403. “[N]early all evidence admissible under Rule 414 will be highly prejudicial.” *United States v. Sanchez*, 440 F. App’x 436, 439 (6th Cir. 2011). Congress nonetheless made the legislative determination that propensity evidence is critical evidence that ordinarily should be admitted in child sex offense cases. *See* 140 Cong. Rec. H8991-92 (“The presumption is in favor of admission. The underlying legislative judgment is that the evidence admissible pursuant to [Rule 414] is typically relevant and probative, and that its probative value is normally not outweighed by any risk of prejudice or other adverse effects.). Courts thus are reluctant to apply Rule 403 stringently to Rule 414 evidence. *See Sanchez*, 440 F. App’x at 439 (warning that Rule 403 should not be used to “gut[]” Rule 414); *United States v. Meacham*, 115 F.3d 1488, 1492 (10th Cir. 1997) (“Rule 403 balancing is still applicable . . . but clearly under Rule 414 the courts are to ‘liberally’ admit evidence of prior uncharged sex offenses”).

In the Fourth Circuit, courts are to engage in a specialized Rule 403 analysis of Rule 414 evidence. They are to apply Rule 403's balancing test by considering at least the following five factors: "(i) the similarity between the previous offense and the charged crime, (ii) the temporal proximity between the two crimes, (iii) the frequency of the prior acts, (iv) the presence or absence of any intervening acts, and (v) the reliability of the evidence of the past offense." *Kelly*, 510 F.4d at 437. Here, the *Kelly* factors overwhelmingly support admitting evidence related to the defendant's uncharged child-pornography-related activity found not to be intrinsic to the charged conduct.

First, the evidence of the defendant's uncharged conduct demonstrates an interest in and method of consuming child pornography that is extremely similar to the government's theory of the defendant's 2015 conduct. Indeed, both the prior conduct and the conduct that led to the defendant's current charges involve his use of P2P programs to access child pornography. Thus, "the similarity between the previous offense and the charged crime," *Kelly*, 510 F.3d at 437, weighs heavily in favor of admission, *see United States v. Rice*, 347 F. App'x 904, 906 (4th Cir. 2009) (holding that prior acts evidence was similar enough for admission in child pornography trial where prior acts involved "showing [a victim] child pornography, as well as taking pictures of [the victim's] genitalia"); *United States v. Majeroni*, 784 F.3d 72, 75–77 (1st Cir. 2015) ("The fact that the prior conduct was similar to the charged conduct enhanced its presumed probativeness.") (collecting cases admitting evidence under Rule 414).

Second, to the extent the defendant's uncharged child-pornography-related activity can be separated from the charged conduct, "the temporal proximity between the . . . crimes" is very small. *Kelly*, 510 F.3d at 437. The roughly three year gap between the defendant's charged conduct and his 2011 to 2012 conduct seems particularly narrow when compared to other cases in

which the Fourth Circuit has affirmed admitting Rule 414 evidence that occurred decades before the charged crimes. *See United States v. Mason*, 532 F. App'x 432, 434 (4th Cir. 2013) (admitting decades-old evidence of molestation in child pornography trial); *Kelly*, 510 F.3d at 437 (finding a twenty-two year intervening period did not render the prior acts inadmissible); *United States v. Emmert*, 825 F.3d 906, 909 (8th Cir. 2016) (finding a twenty year intervening period to be acceptable); *United States v. Carino*, 368 F. App'x 929, 929 (11th Cir. 2010) (admitting, in child pornography trial, decades-old evidence that the defendant molested his younger sister when he was sixteen); *United States v. Eiker*, 2:17-CR-72 (MSD) 2017 WL 6459510, at \*1–6 (noting that “the intervening period between alleged prior acts and the instant charges—somewhere between eleven and twenty-one years—does not render the prior acts inadmissible”).

Third and fourth, “the frequency of the prior acts,” and “the presence or absence of any intervening acts” cut in favor of admission. As noted, the defendant’s efforts to obtain and view child pornography discussed in the Notice under Rule 414 occurred in some instances just a few years before the crimes charged, and there is no evidence of intervening acts that would render this evidence less probative or reliable.

Finally, the evidence of the defendant’s prior child-pornography-related activity is extremely reliable. The defendant himself admitted to engaging in the 2010 and 2015 conduct and, as explained above and in the government’s Notice of Intent to Introduce Certain Evidence Pursuant to Federal Rule of Evidence 414, *see* Dkt. 43, the forensic examination of the Dell laptop seized from the defendant’s home uncovered compelling evidence that the defendant used the device to search for, download, and view child pornography. The reliability of the proffered evidence thus weighs in favor of its admission.

As the cases cited above demonstrate, courts typically find that the 403-balancing test favors admissibility of Rule 414 evidence, even if the Rule 414 evidence is decades-old. *See, e.g.*, *Rice*, 347 F. App'x at 906 (admitting in child pornography trial testimony of live victim regarding decades-old abuse involving distribution and production of child pornography). This trend is not surprising since “Rule 414 reflects Congress’s view that,” when it comes to sexual offenses, “propensity evidence is typically relevant and probative.” *United States v. Haney*, 693 F. App'x 213, 214 (4th Cir. 2017) (quoting *Kelly*, 510 F.3d at 437). While all Rule 414 evidence carries some inherent prejudice, courts have repeatedly held that it is the type of prejudice contemplated by Congress and thus should not be considered unfair prejudice under Rule 403. *See Rice*, 347 F. App'x at 906 (noting that “past ‘sexual abuse [evidence] was certainly prejudicial to Rice’s defense, it was not *unfairly* prejudicial.’ Instead, ‘it was prejudicial for the same reason it is probative’ it tends to prove that Rice has a deviant sexual attraction towards children” (quoting *Kelly*, 510 F.3d at 438) (emphasis in original)). Moreover, where, as here, the Rule 414 evidence is similar to the crimes charged, courts have found that the evidence adds little marginal prejudice. *See Eiker*, 2017 WL 6459510, at \*3 (noting that “while the prior acts here are clearly disturbing, they do not have a strong danger of causing unfair prejudice because they concern similar types of sexual exploitation to those for which Defendant has been charged”).

**C. The Uncharged Child Pornography Offenses Are Admissible Under Rule 404(b) to Show Identity, Knowledge, Opportunity, Intent, and Lack of Mistake**

Even if this evidence was not intrinsic to the government’s charges, and even if Rule 414 did not apply, the defendant’s uncharged child pornography offenses, and all of the child pornography found on the defendant’s devices, are nevertheless admissible under Rule 404(b) as “relevant to an issue other than character, such as identity or motive.” *United States v. Blauvelt*, 638 F.3d 281, 292 (4th Cir. 2011). Rule 404(b)’s prohibition on the introduction of “[e]vidence

of a crime, wrong, or other act” applies only where the purpose of such evidence is “to prove a person’s character in order to show that on a particular occasion the person acted in accordance with the character.” For Rule 404(b) to apply, the other acts evidence must be “extrinsic to the [conduct] charged.” *United States v. Basham*, 561 F.3d 302, 326 (4th Cir. 2009) (internal quotations and citation omitted). That is, prior bad acts “intrinsic to the alleged crime do not fall under Rule 404(b)’s limitations on admissible evidence.” *Id.* (internal quotation and citation omitted). Rule 404(b) thus has no application to evidence of uncharged conduct that “arose out of the same series of transactions as the charged offense,” “is necessary to complete the story of the crime on trial,” or “is necessary to provide context relevant to the criminal charges.” *Id.* (internal quotations and citation omitted). Likewise, Rule 404(b)’s limitations do not apply to evidence of uncharged conduct that is “inextricably intertwined,” “part of a single criminal episode,” or “were necessary preliminaries to the crime charged.” *United States v. Chin*, 83 F.3d 83, 88 (4th Cir. 1996).

Even if other acts evidence is “extrinsic” to the crime charged, such evidence may still be admitted consistent with Rule 404(b). As the Fourth Court has observed, Rule 404(b) is “an inclusive rule, admitting all evidence of other crimes or acts except that which tends to prove only criminal disposition.” *Basham*, 561 F.3d at 326 (internal quotations and citation omitted). So long as the proffered bad acts are relevant to an issue other than the defendant’s character—such as ““proof of motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident,”” *Basham*, 561 F.3d at 326 (quoting Fed. R. Evid. 404(b))—and the threshold requirements of Rule 404(b) are met, then evidence of the other bad acts is admissible. *Morgan*, 846 F.2d at 944.

The Fourth Circuit has developed a four-pronged test to protect against the dangers Rule 404(b) is intended to address. *See United States v. Johnson*, 617 F.3d 286, 296–97 (4th Cir. 2010). Evidence of prior bad acts becomes admissible under Rule 404(b) and Rule 403 if it meets the following criteria:

(1) The evidence must be relevant to an issue, such as an element of an offense, and must not be offered to establish the general character of the defendant. In this regard, the more similar the prior act is (in terms of physical similarity or mental state) to the act being proved, the more relevant it becomes. (2) The act must be necessary in the sense that it is probative of an essential claim or an element of the offense. (3) The evidence must be reliable. And (4) the evidence’s probative value must not be substantially outweighed by confusion or unfair prejudice in the sense that it tends to subordinate reason to emotion in the factfinding process.

*Id.* (quoting *United States v. Queen*, 132 F.3d 991, 997 (4th Cir. 1997)). The threshold for relevancy and necessity are not high. Relevancy requires only that the evidence be “worth consideration by the jury” or have a “plus value” to be admissible. *Queen*, 132 F.3d at 998. As for necessity, prior acts evidence is considered necessary where, “considered in the light of other evidence available to the government, it is an essential part of the crimes on trial, or it furnishes part of the context of the crime.” *Id.* (internal quotations and citation omitted). Where intent is at issue and the Rule 404(b) evidence is important to the proof of intent, the evidence may be considered necessary. *Id.*

Any and all extrinsic evidence of prior, uncharged child pornography offenses and the child pornography found on the defendant’s devices are highly relevant to the charged conduct because they show motive (that the defendant had an intense desire to receive and possess child pornography), and hence identity (that it was likely the defendant and not anyone else who downloaded the child pornography onto the defendant’s computer). *See United States v. Sebolt*, 460 F.3d 910, 917 (7th Cir. 2006) (“Prior instances of sexual misconduct with a child victim may establish a defendant’s sexual interest in children and thereby serve as evidence of the

defendant's motive to commit a charged offense involving the sexual exploitation of children."); *Eiker*, 2017 WL 6459510, at \*3 ("Defendant's prior acts demonstrate an interest in prepubescent girls, and the images described as forming the basis for Counts 1–3 show victims engaged in sexual conduct similar to that of the prior acts.").

Motive to download child pornography is especially relevant because such a desire does not exist in the overwhelming majority of the population. *See United States v. Hawpetoss*, 478 F.3d 820, 824 (7th Cir. 2007) ("In child molestation cases, for example, a history of similar acts tends to be exceptionally probative because it shows an unusual disposition of the defendant ... that simply does not exist in ordinary people."). The likelihood that someone sharing the defendant's sexual interest in child exploitation material may have had repeated, unsupervised access to the defendant's computer is vanishingly small. Therefore, any extrinsic evidence of uncharged child pornography offenses, and any child pornography, combined with other evidence the government intends to offer at trial, will show that the defendant was the only person with the motive and opportunity to commit the charged crimes. *See United States v. Siegel*, 536 F.3d 306, 317–18 (4th Cir. 2008) (admitting evidence of past crimes to show motive for murder).

Evidence of the uncharged child pornography offenses, and all of the found child pornography, are also highly relevant to show that the defendant received and possessed the charged child pornography knowingly and not by mistake. "A not-guilty plea puts one's intent at issue and thereby makes relevant evidence of similar prior crimes when that evidence proves criminal intent." *United States v. Sanchez*, 118 F.3d 192, 196 (4th Cir. 1997). Thus, even outside the child pornography context, courts routinely admit similar prior bad acts to show that the charged conduct was committed intentionally. *See, e.g., id.* at 195–96 (evidence of prior drug dealing admissible to show defendant was an "intentional, rather than unwitting, participant in the

conspiracy”); *United States v. Ford*, 88 F.3d 1350, 1362 (4th Cir. 1996) (prior drug arrest admissible to show intent to distribute narcotics); *United States v. Tanner*, 61 F.3d 231, 237 (4th Cir. 1995) (same); *United States v. Aguilar-Aranceta*, 58 F.3d 796, 799 (1st Cir. 1995) (“Where the evidence is susceptible to the explanation that the acts alleged to constitute the crime were innocently performed and the crucial issues of intent and knowledge are keenly disputed, . . . the government [may] introduce evidence of prior or similar offenses . . . .”). Just as a defendant’s prior drug possession or sale is relevant to show that his possession of the charged narcotics was likely no accident, so too is prior evidence of a defendant’s intentional receipt, attempts to receive, and possession of child pornography. *See United States v. Knope*, 655 F.3d 647, 657 (7th Cir. 2011) (holding that the defendant’s “expressed interest in having sex with minors in the past” and his attempt “to meet with at least one minor for this purpose . . . was relevant to establishing Knope’s knowledge, intent, and lack of mistake”); *United States v. Miller*, 688 F.3d 322, 329–30 (7th Cir. 2012) (“This evidence was probative of Miller’s intent to view images of naked children and that his doing so was no mistake.”).

## **II. The Court Can Determine that the Child Pornography Depicts Real Minors Engaged in Sexually Explicit Conduct**

Notwithstanding any related evidence the government may introduce at trial, the Court is capable of determining on its own that the proffered images of child pornography depict real victims under the age of 18. “Although the Fourth Circuit has yet to rule upon the issue, other circuits have concluded that images themselves may be sufficient evidence for a jury to conclude that real children are depicted.” *United States v. Doyle*, 621 F. Supp. 2d 337, 340 (W.D. Va. 2009) (citing *United States v. Salcido*, 506 F.3d 729, 733–34 (9th Cir. 2007); *United States v. Rodriguez-Pacheco*, 475 F.3d 434, 437 (1st Cir. 2007); *United States v. Irving*, 452 F.3d 110, 121–22 (2d Cir. 2006); *United States v. Farrelly*, 389 F.3d 649, 654 & n.4 (6th Cir. 2004), abrogated on other

grounds by *United States v. Williams*, 411 F.3d 675, 678 n.1 (6th Cir. 2005); *United States v. Slanina*, 359 F.3d 356, 357 (5th Cir. 2004); *United States v. Kimler*, 335 F.3d 1132, 1142 (10th Cir. 2003); *United States v. Deaton*, 328 F.3d 454, 455 (8th Cir. 2003). The factfinder, in other words, can determine for itself whether a child is real and under the age of 18. Not requiring the government to call a witness to establish this fact is particularly appropriate where, as here, the images unambiguously depict children under the age of 18.

## CONCLUSION

For the forgoing reasons, the government respectfully submits that, upon the conclusion of this trial, it will have proven the defendant's guilt on all counts beyond a reasonable doubt.

Respectfully submitted,

G. Zachary Terwilliger  
United States Attorney

Date: August 28, 2019

By: \_\_\_\_\_/s/  
William G. Clayman  
Special Assistant United States Attorney (LT)  
Carina A. Cuellar  
Assistant United States Attorney  
United States Attorney's Office  
2100 Jamieson Ave.  
Alexandria, Virginia 22314-5794  
Phone: 703-299-3700  
Fax: 703-299-3981  
Email: william.g.clayman@usdoj.gov  
Email: carina.cuellar@usdoj.gov

**CERTIFICATE OF SERVICE**

I hereby certify that on this day, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will then send a notification of such filing (NEF) to counsel of record for the defense.

By: /s/

William G. Clayman  
Special Assistant United States Attorney (LT)  
United States Attorney's Office  
2100 Jamieson Ave.  
Alexandria, Virginia 22314-5794  
Phone: 703-299-3700  
Fax: 703-299-3981  
Email: william.g.clayman@usdoj.gov